10 Sigillum KeySign

Application Notes CrypToken®

Document Protection Signing Documents

Described Version:	KeySign 2.2.11
Also applicable for:	KeySign 2.0 and higher
Target platforms:	Windows Vista 32/64 /XP/2000
MARX hardware:	CrypToken® M2048 and MX2048 JCOP

True Digital Signature and Document Protection!

With the increasing reliance on the Internet for transfer of critical business information, authenticity and integrity of documents becomes more and more important. Microsoft Office allows digital signing of documents to verify the authors identity and to ensure that the document was not changed. With the CrypToken® it is possible to store certificates on a mobile and secure USB token. Thereby your certificates are with you wherever and whenever you need them.

- **Easy Integration of the CrypToken**
- **Multiple signatures for one document**
- **Authentication with X.509 certificates**
- **Guarantees integrity of documents**

MARX® CryptoTech®

Mobilize your Authentication!

www.cryptoken.com

10_31May007_rd/AN_KeySign.indd

Table of Contents

1. Requirements

- Microsoft Windows (Vista 32/64, XP, 2000)
- Installed Sigillum KeySign
- CrypToken M2048 (Raak*Sign*), CrypToken M2048 (MARX Middleware, MS-CAPI formatted) or CrypToken 2000 (with MS-CAPI Partition)

2. CrypToken® Installation

2.1 CrypToken® M2048 with Raak*Sign*® Middleware

Driver Installation

Attach the CrypToken to any USB port. Windows will notify a new device and opens the Found New Hardware Wizard. Follow the instructions of the wizard. For driver location choose the folder \driver on the CrypToken Security Kit CD or download the latest version at www.cryptoken.com/support.

Under Windows XP, 2000, 2003 Server, Me and 98 it is recommended to install the Hot Plug Enabler (static driver) that is located \Drivers\WinXP-2000-2003Server-Me-98\Hot Plug Enabler. To do so run setup.exe and follow the instructions of the installation wizard.

Raak*Sign*® Middleware

To install Raak*Sign* run the setup.exe at \Middleware (Windows)\Administrator Installation on the CD and follow the instructions of the installation wizard.

For more information read the installation guide: \Middleware (Windows)\RaakSign Installation.pdf

2.2 CrypToken® M2048 with MARX® Middleware, CrypToken® 2000

2.2.1 Automatic Installation with CSPSetup

CSPSetup.exe is part of the CrypToken Security Kit and processes following steps:

- CrypToken device drivers
- CrypToken CSP components for PKCS#11 and MS-CAPI
  - Copies PKCS#11 DDL to C:\Windows\System32\PKCS_MARX.DLL
  - Copies MS-CAPI DLL to C:\Windows\System32\CSP_MARX.DLL
  - Registers MS-CAPI DLL
- MARX Security Center in Windows System Tray for quick access to CrypToken applications (Installation folder: C:\Program Files\Common Files\MARX Shared)
- SSO (Single SignOn) component for PIN caching, which ensures that end user does not need to enter the CrypToken PIN continuously every time the CrypToken is accessed by an application through MARX CSP (Cryptographic Service Provider).
- MARX Explorer for managing attached CrypTokens and examining certificates stored on it.

To install MARX CSP run CSPSetup.exe that is located in the root directory of the CrypToken Security Kit CD. Follow the instructions of the installation wizard.

2.2.2 Manual Driver and CSP Installation

Driver Installation

For manual installation attach the CrypToken to any USB port. Windows will notify a new device and opens the Found New Hardware Wizard. Follow the instructions of the wizard as shown in figure 2.1 and 2.2. For driver location choose the folder \files\driver on the CrypToken Security Kit CD or download the latest version at www.cryptoken.com/support

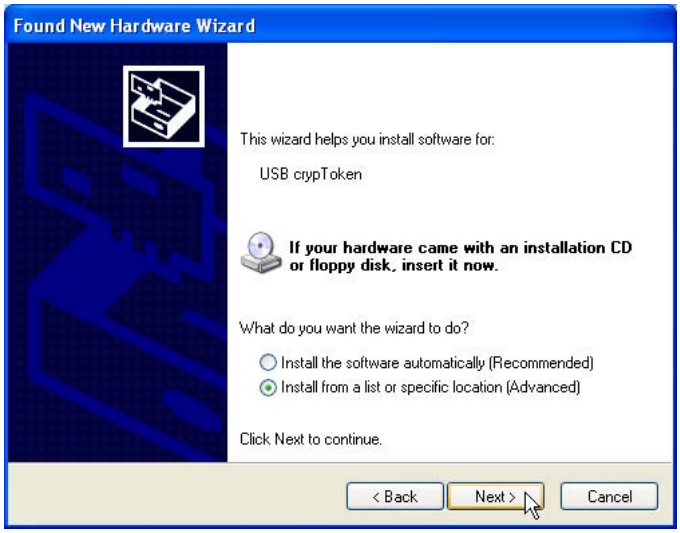


Fig. 2.1: Found New Hardware Wizard (Step 1 and 2 - Win XP)

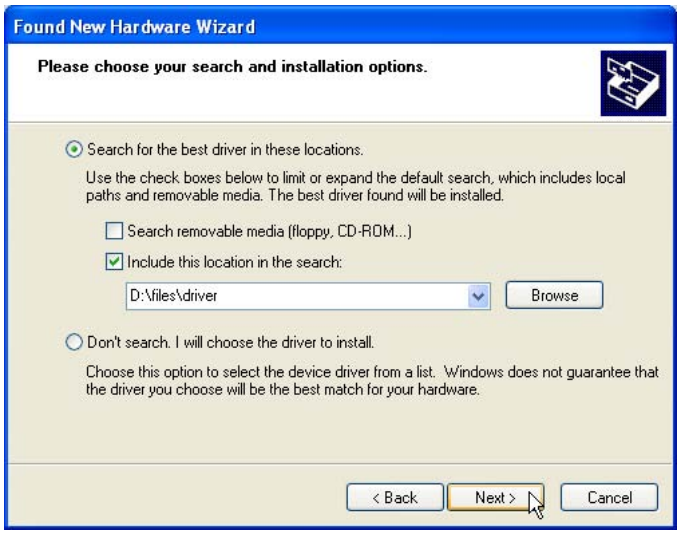


Fig. 2.2: Found New Hardware Wizard (Step 2 and 3 - Win XP)

For CrypToken 2000 it is also possible to install drivers with CTSetup.exe from the CT-Kit CD-ROM \files\driver

MS-CAPI

To install MS-CAPI for CrypToken run files\CSP\Install.bat on the CT-Kit CD-ROM.

3. Certificate Management

3.1 CrypToken® M2048 with Raak*Sign*® Middleware

Storing Certificates on the CrypToken

Attach the CrypToken to your computer and run the Token Administration Utility that was installed together with the Raak*Sign* Middleware. Go to "Digital IDs" and select "Import Digital ID" or "Import Certificate" depending on the extension of your certificate file.

Select "Import Digital ID" for

- .pfx
- .p12

or "Import Certificate" for

- .cer
- .der

Afterwards browse to your certificate file and enter its password. RaakSign Administration Utility will prompt for the CrypToken PIN on the next screen. You will get a notification after the certificate was successfully stored.

Backup Certificates

Your digital certificate comprises a public part containing a public key and a digital signature, with an accompanying private key. The certificate does not work without the private key. That is why it is vital to take good care of the private key.

After applying for a certificate you will receive an encrypted file. That file contains the public part signed by the CA and the private key. MARX recommends to copy the certificate file to a removable media (floppy disk, CD, USB storage drive etc.) and keep it in a safe location. This allows you to restore the certificate from the backup, should the original be lost or deleted.

It is not possible to backup certificates that are stored on the CrypToken. Please take this into account before deleting the original certificate file.

3.2 CrypToken® M2048 with MARX® Middleware, CrypToken® 2000

Storing Certificates on the CrypToken

To store a certificate, attach the CrypToken to your computer and double-click on the certificate file you received from the Certificate Authority (e.g. certificate.p12). Windows will start the "Certificate Import Wizard". The proper path to the certificate file will be inserted automatically. Otherwise browse to the certificate file you want to import.

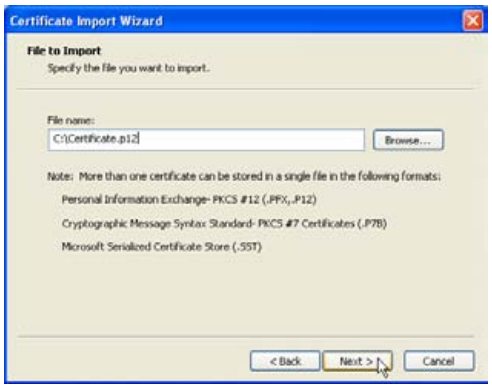
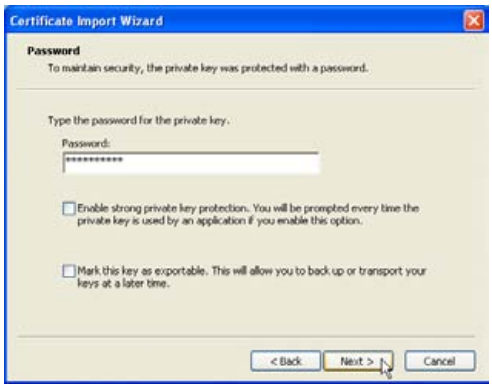


Fig. 3.1: Certificate Import Wizard

Fig. 3.2: Enter certificate file name

The wizard will ask you for the certificate file password and start searching for different certificate stores. Please enter the CrypToken PIN and confirm. For the Evaluation Version the PIN is "demo". If you already received a customer specific CrypToken you will find the PIN (User Password) on your Production Sheet.



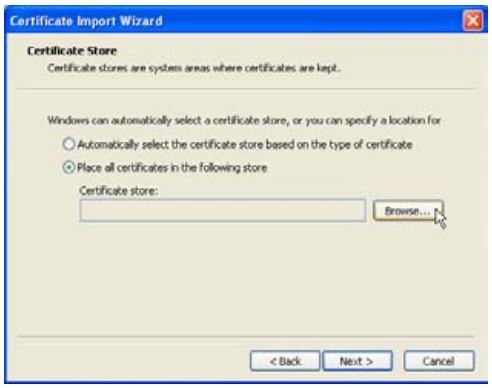


Fig. 3.3: Enter password of the certificate file

Fig. 3.4: Select certificate storage

Click on "Show physical stores" and browse to "Personal" ⇨ "crypToken" (Fig. 3.5) and confirm by clicking on "OK".

Fig. 3.5: Select crypToken

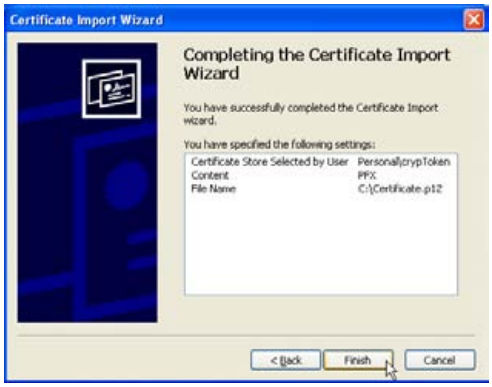


Fig. 3.6: Confirm CrypToken as certificate storage

Fig. 3.7: Completing the certificate import

Click on "Finish" to store the certificate on the CrypToken. The wizard will notify you that the certificate was successfully imported.

Backup Certificates

Your digital certificate comprises a public part containing a public key and a digital signature, with an accompanying private key. The certificate does not work without the private key. That is why it is vital to take good care of the private key.

After applying for a certificate you will receive an encrypted file. That file contains the public part signed by the CA and the private key. MARX recommends to copy the certificate file to a removable media (floppy disk, CD, USB storage drive etc.) and keep it in a safe location. This allows you to restore the certificate from the backup, should the original be lost or deleted.

It is not possible to backup certificates that are stored on the CrypToken. Please take this into account before deleting the original certificate file.

4. Signing Documents

Signing is the last step while creating a document because later changes will cause that the document is no longer signed.

Start the Windows Explorer and browse to the file that has to be signed. Click on the file using the right mouse button and select "KeySign Professional" (Fig. 4.1).

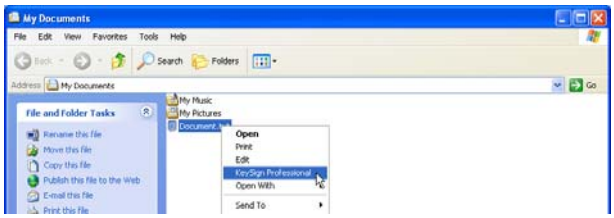


Fig. 4.1: Select "KeySign Professional"

KeySign will open the document. Check the content of the file and click on the "Sign..." button (Fig. 4.2).

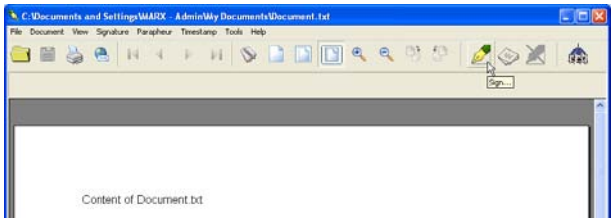


Fig. 4.2: Start signing

The "Signature Dialog" will open. Click on "Select..." and choose the certificate that has to be used to sign the document. Afterwards enter a declaration (if required) and click on "Sign" to add the signature (Fig. 4.3).

Fig. 4.3: Open "Select certificate" dialog

KeySign will ask you for the PIN of the CrypToken. Now your digital signature appears in the list of all persons who signed the document. Signed documents can be identified by the certificate symbol (Fig 4.4).

Fig. 4.4: Signed document

The last step is to store the document. To do so, click on "File" ⇨ "Save". The document will be saved as .sfx file.

Appendix

Appendix A - Distributors

USA

MARX CryptoTech LP
4485 Tench Rd. #310
Peachtree Commons Office Park
Suwanee, GA 30024
U.S.A.
www.cryptoken.com

Sales: sales@cryptotech.com
Support: support@cryptotech.com
Phone: (+1) 770-904-0369
Fax: (+1) 770-904-3893
Email: info@cryptotech.com

Germany

MARX Data Security GmbH
Vohburger Strasse 68
D-85104 Wackerstein
Germany
www.cryptoken.com

Sales: sales@cryptoken.com
Support: support@cryptoken.com
Phone: +49 (0) 8403 9295 14
Fax: +49 (0) 8403 9295 29
Email: contact@cryptoken.com

Poland

Microplan Polska Sp. z o.o.
Polwiejska 3
PL-61-885 Poznan
Poland
www.microplan.pl

Sales: Gregor Bigos
Phone: +48 (0) 61 8518916
Fax: +48 (0) 61 8518774
Email: big@microplan.pl

Appendix B - CrypToken Certifications and MARX Memberships